ABSTRACT OF THE DISCLOSURE

The present invention provides an apparatus and method for performing cryptographic operations on a plurality of input data blocks within a processor. In one embodiment, an apparatus for performing cryptographic operations is provided. The apparatus includes a cryptographic instruction, CFB mode logic, and execution logic. The cryptographic instruction is received by a computing device as part of an instruction flow executing on the computing device. The cryptographic instruction prescribes one of the cryptographic operations. The one of the cryptographic operations includes a plurality of CFB block cryptographic operations performed on a corresponding plurality of input text blocks. The CFB mode logic is operatively coupled to the cryptographic instruction. The CFB mode logic directs the computing device to update pointer registers and intermediate results for each of the plurality of CFB block cryptographic operations. The execution logic is operatively coupled to the CFB mode logic. The execution logic executes the one of the cryptographic operations.